RSAC 2025 Conference

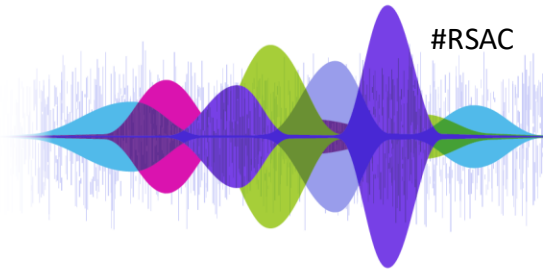
Many Voices.
One Community.

SESSION ID: CTF-T09

Cloud CTF 201: Solving Capture-The-Flag Challenges in AWS, Azure, GCP

Jenko Hwong
Threat Research
WideField Security

Luis Rivas
Network System Engineer
Department of Defense



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The views and opinions expressed in this presentation are solely those of the speaker and do not represent the views, policies, or positions of the Department of Defense (DoD), the U.S. Army, or any other government agency. This presentation is made in the speaker's personal capacity and does not constitute an endorsement by the DoD or the U.S. Army.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

MEET THE TEAM

> WHOAMI

Many Voices.
One Community.

Meet the team

Jenko Hwong

linkedin: jenkohwong

- Cloud threat research, products and engineering
- Vulnerability management, pen-testing, threat intel, AD security
- Contributor Cloud Village CTF

Luis Rivas

GitHub: G0TH3R

- Cybersecurity Researcher and experienced Red Teamer
- Works, learns, and mentors @ Cloud Village
- Over 10 years working with IT, Cybersecurity, and hacks

Agenda

What are we doing here?

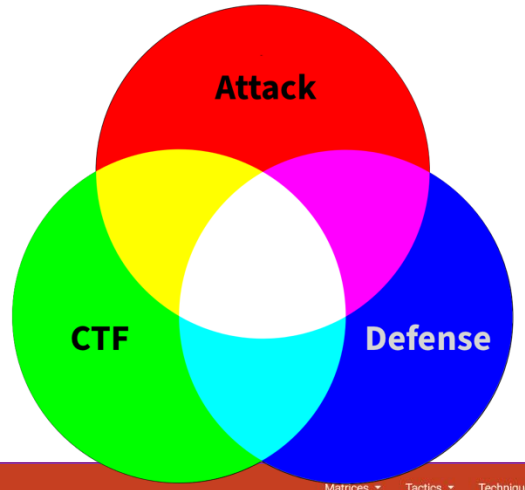
→ Introduction: Meet The Cloud Threat

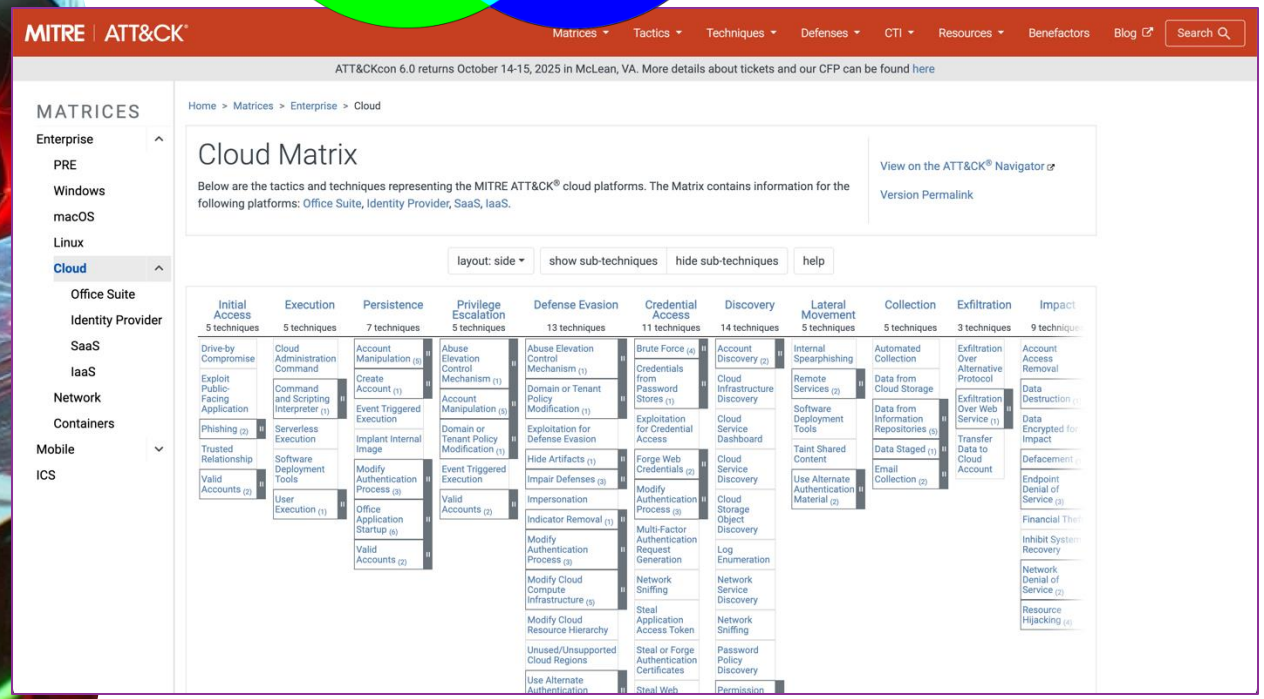
→ Set your env

→ Solving the Challenge

→ Apply what you learned!

Meet the Cloud Threat





Using a common framework

RSAC™ 2025 Conference

AWS

Threat Actor:
APT-909 "Nebula Specters"

Cloud-native adversary targeting DevOps pipelines, cloud IAM misconfigurations, and ephemeral credentials.

Tactics & Techniques:

- **T1087.004** - Cloud Account Discovery
- **T1552.005** - Unsecured Credentials in Instance Metadata Service
- **T1078.004** - Cloud Accounts with Misconfigured Role Assumption

Objective:

(C) Persistence & Data Exfiltration from AWS

Set your environment

env

```
→ curl https://github.com/cloud-village/rsac-2025-lab

→ Instructions to start your journey: $M4NAG3R or $H4CK3R
```

CHOOSE YOUR ADVENTURE

Solving the Challenge: AWS

→

→

→

→ AWS Challenge << EOF > solution.md

BLOG // TECH // SEP 13, 2022
Introducing: CloudFox
By: Seth Art, Alumnus Principal Security Consultant & Carlos Vendramini, Bishop Fox Alumnus
cloudfox

Choose your Tools!

~ Exploiting EC2 Instance Metadata for Temporary Credentials

→ cat AWS_Challenge_1.txt

→ **Scenario:** A misconfigure EC2 instance allows APT 909 metadata service (IMDSv1) access.

→ **Goal:** Extract Temporary AWS Credentials.

→ Technique: Abuse EC2 Metadata API

Defensive Measures:
Enforce IMDSv2, restrict IAM roles, monitor VPC Flow Logs

→ cat AWS_Challenge_2.txt

→ **Scenario:** The attacker gains access to an IAM user token from a compromised developer's laptop.

→ **Goal:** Extract AWS account details and discover privilege escalation paths.

→ Technique: Enumerate IAM Roles & Permissions

Defensive Measures:
CloudTrail logging, IAM least privilege, GuardDuty alerts.

~ Privilege Escalation and Data Exfiltration

→ cat AWS_Challenge_3.txt

→ **Scenario:** The attacker finds an overprivileged IAM role that allows sts:AssumeRole and access to S3 bucket.

→ **Goal:** Move laterally by assuming a more privileged role and exfil data.

→ Technique: IAM Role Hijacking and S3 Accessible S3 Buckets

Defensive Measures:
Restrict sts:AssumeRole, enable CloudTrail and bucket monitoring

RSAC 2025 Conference

GCP

Threat Actor:
UNC-225 "Evil Corp"

Cloud-native adversary targeting DevOps pipelines, cloud IAM misconfigurations, and ephemeral credentials.

Tactics & Techniques:

- **T1486.000** – Data Encrypted for Impact
- **T1552.005** - Unsecured Credentials in Instance Metadata Service
- **T1078.004** - Cloud Accounts with Misconfigured Role Assumption

Objective:

(C) Persistence & Data Exfiltration from GCP

Set your environment

env

```
→ curl https://github.com/cloud-village/rsac-2025-lab

→ Instructions to start your journey: $M4NAG3R or $H4CK3R
```

CHOOSE YOUR ADVENTURE

```
→
→
→
→ GCP Challenge << EOF > solution.md
```

~ Supply Chain Attack via Cloud Build Poisoning

→ cat GCP_Challenge_1.txt

→ **Scenario:** A DevOps pipeline in Cloud Build is injected with malicious artifacts.

→ **Goal:** Inject a backdoored artifact into Cloud Build to gain access.

→ Technique: Cloud Build Privilege Escalation & Artifact Poisoning

Defensive Measures:

- Monitor for unauthorized Cloud Build Modifications
- Limit Cloud Build to only necessary permissions
- Enforce Binary Authorization to prevent unsigned deployments

~ Escaping a GKE Container to Compromise the Host

→ cat GCP_Challenge_2.txt

→ **Scenario:** A **cluster** allows attackers to **escape and** gain **host-level.**

→ **Goal:** Exploit **GKE misconfigurations** to escape a container and execute commands on the underlying host.

→ Technique: Kubernetes privilege Escalation + Escape to Host

Defensive Measures:
Pod Security Policies: Prevent containers from running as root.
Restrict Kubernetes RBAC: Ensure least privilege
Cloud Logging: Monitor unusual Kubernetes API calls

RSAC™ 2025 Conference

Azure

Threat Actor: Storm-2025 "Rosa Klebb"

Cloud-native adversary targeting OAuth tokens, service principals, and native services.

Tactics & Techniques:

- **T1550.001** – Application Access Token
- **T1556.009** – Conditional Access Policies
- **T1078.004** - Cloud Accounts

Objective:

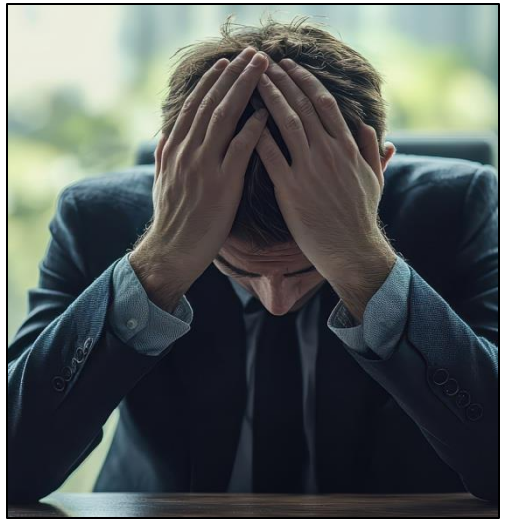
(C) Defense Evasion & Persistence

Set your environment

env

```
→ curl https://github.com/cloud-village/rsac-2025-lab

→ Instructions to start your journey: $M4NAG3R or $H4CK3R
```



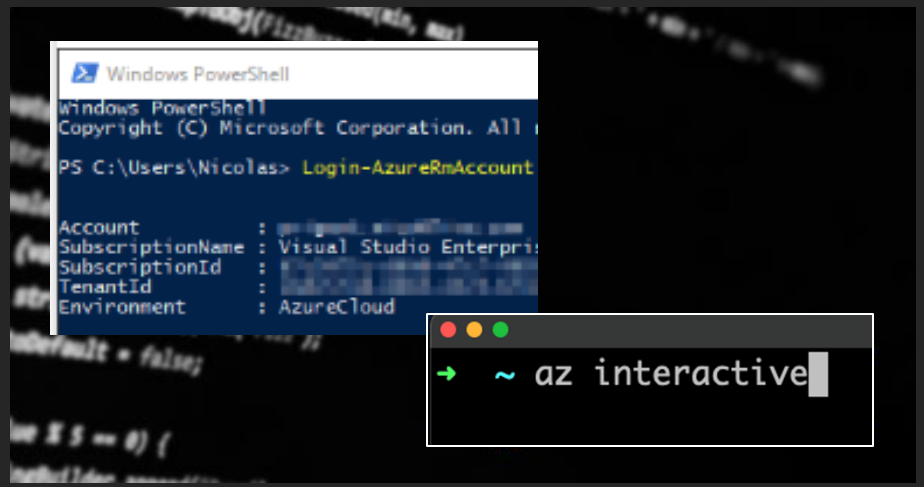
CHOOSE YOUR ADVENTURE

→

→

→

→ Azure Challenge << EOF > solution.md



Choose your Tools!

~ Privilege Escalation and Data Exfiltration

→ cat Azure_Challenge_1.txt

→ **Scenario:** Weak authentication policies lead to session hijacking and access.

→ **Goal:** Enumerate users, password-spray, discover targets, spear-phish.

→ Technique: Use enumeration and password spray, MSGraph calls, and device code phish.

Defensive Measures:
Entra ID hardening, user types, MFA, and Conditional Access.

~ Privilege Escalation and Data Exfiltration

→ cat Azure_Challenge_2.txt

→ **Scenario:** Service principals allow privilege escalation.

→ **Goal:** Exploit App Administrator access to gain control of an SP.

→ Technique: az ad sp, aadinternals

Defensive Measures:
Restricted roles, strong SP auth, Azure log monitoring.

~ Privilege Escalation and Data Exfiltration

→ cat Azure_Challenge_3.txt

→ **Scenario:** Post access, you want to install backdoors for persistence.

→ **Goal:** Use temporary delete status, Cloud Shells, service principals, and Serverless functions for persistence.

→ Technique: custom

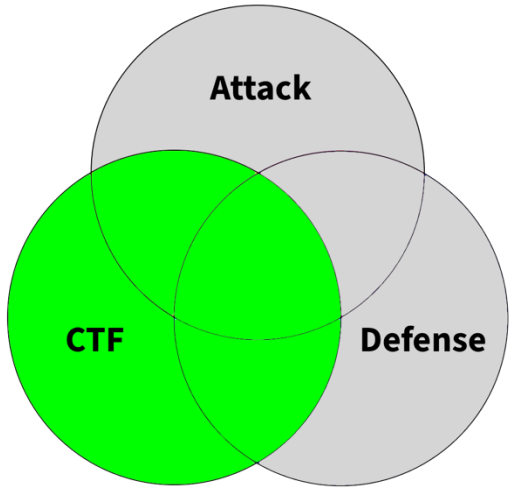
Defensive Measures:
Restricted roles, strong SP auth, Azure log monitoring.

RSAC 2025 Conference

Learnings

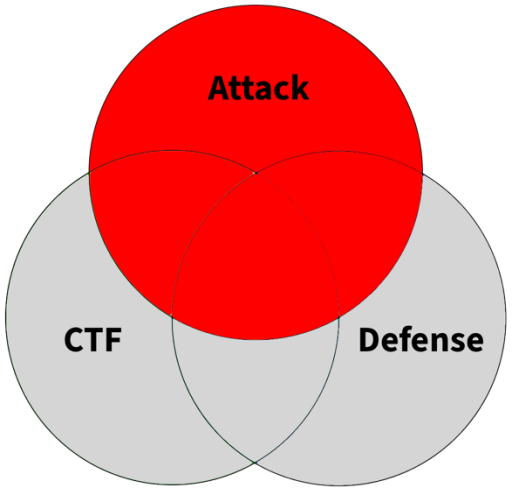
“Apply” CTF in Life

- CTF is a playground
  - Sharpen your skills in CTFs
  - Seek out and share knowledge
  - Have fun and learn
- The office is the battleground
  - Map to real red-team techniques
  - Anticipate defensive measures as you solve challenges
  - Teamwork



“Apply” the Adversarial Perspective

- The ignored attack chain
  - Enumeration and discovery are ignored
  - Persistence is not just a good red-team trait
  - Cloud log evasion and confusion
- Techniques
  - Session tokens are a gift that keeps giving
  - Confused identities are an opportunity
- “Know thy adversary”
  - IPs, domains, URLs – exploit the trust and hide in the noise
  - Posture/config, MFA, conditional access, primary credentials



“Apply” Defense in Depth

- Cybersecurity is everyone’s realm

  Protect it.

- Learn more about attacks – Understand how to defend

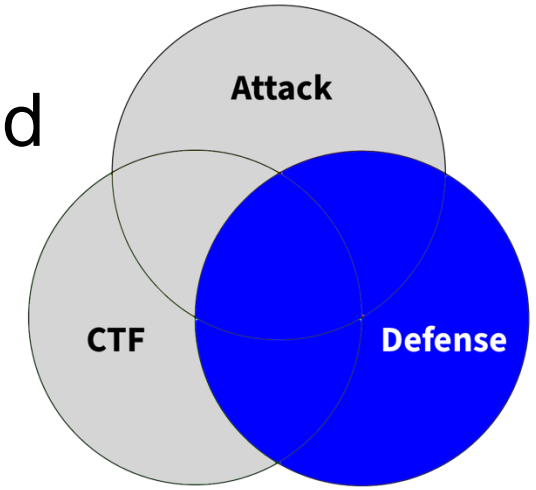
  Zero Trust will not defend itself.

- Analyze broadly

  Implement incrementally.

- Some defense is better than NO Defense

  You are ready.



RSAC 2025 Conference

Resources

Code and Explanations

- https://github.com/cloud-village/rsac-2025-lab

```
README.md
Technical_Notes.pdf
Solutions.pdf
AWS/
Azure/
GCP/
Tools/
```

RSAC™ | 2025 Conference

Many Voices.
One Community.